ABSTRACT OF THE DISCLOSURE

Disclosed is a modular multiplication apparatus for high-speed encryption/decryption and electronic signature in a mobile communication environment including smart cards and mobile terminals. The present invention provides an apparatus for performing Montgomery type modular multiplication for calculating $A \cdot B \cdot R^{-1} \bmod N$ (where $R=4^{m+2}$) in m+2 (where m=n/2) clocks with the multiplier A and the multiplicand B, each having n bits as its inputs, wherein bits of the multiplier are sequentially shifted to generate a shifted bit string and the two least significant bits of the generated bit string are Booth-recorded. The present invention provides a high-speed modular multiplication apparatus with fewer gates and reduced power consumption.